News from Ed Markey

United States Congress **Massachusetts Seventh District**

FOR IMMEDIATE RELEASE
August 22, 2003

CONTACT: Michal Freedhoff
or Israel Klein
(202) 225-2836

DID CYBER WORM INFECT FIRSTENERGY NUCLEAR PLANT ON EVE OF BLACKOUT?

Lawmaker Probes Implications of Computer Virus Crashing Nuclear Safety System in January

Washington, DC: Representative Edward J. Markey (D-MA), a senior Member of the House Energy and Commerce and Homeland Security Committees, today released a letter to the Nuclear Regulatory Commission (NRC) asking whether cyber-security flaws at FirstEnergy may have contributed to last week's widespread blackout. In January 2003, a computer virus was able to penetrate a private computer network at FirstEnergy's Davis-Besse nuclear power plant in Ohio. Just prior to last week's blackout, another computer virus – the so-called Blaster worm -- was at its peak level of activity, which raises the possibility that perhaps cyber-security weaknesses at the FirstEnergy Davis-Besse (or other) power plant may have been a contributing factor.

"We are dependent on a reliable electricity grid to power our economy, yet it is appears that the utility at the center of last week's blackout has a record of cyber-security lapses that could make us all vulnerable. The American people deserve to know that their lights, telephones, water supplies, and emergency response systems are protected by the highest level of firewalls and anti-hacker oversight. Just a few short months ago, cyber-security was so bad at the Davis-Besse reactor that a worm zipped right into a key safety monitoring system and crashed it," said Rep. Markey. "We need to know whether FirstEnergy was following cyber-security regulations at the time, whether the problems at Davis-Besse and other power plants after the January worm attack were corrected, and whether a virus-compromised network contributed in any way to last week's power outage," said Rep. Markey.

Press reports have indicated that in January 2003, the Slammer worm entered the Davis-Besse plant by penetrating the unsecured network of a Davis-Besse contractor, and then proceeded through a T1 line that bridged that network and Davis-Besse's corporate network. The T1 line turned out to be one of several that completely bypassed the company's firewall. The Slammer worm was reported to be the fastest spreading computer worm in history, infecting more than 90% of vulnerable hosts within 10 minutes, and causing network outages, cancelled flights, and ATM failures. By 4 PM, nuclear power plant workers noticed a slowdown on the plant network. At 4:50 PM, the congestion created by the worm crashed the plant's computerized display panel (the Safety Parameter Display System, or SPDS), and at 5:13 PM, the Plant Process Computer (PPC) crashed. It took 4 hours and 50 minutes to restore the SPDS and 6 hours and 9 minutes to restore the PPC. Press reports have also indicated that the Slammer worm penetrated and seriously disabled other utility companies' networks.

Rep. Markey's letter asked for information related to:

- Whether the NRC has promulgated new cyber-security regulations both since September 11 and since the January 2003 worm attack at Davis-Besse, and whether cyber-security at nuclear power plants is adequately evaluated.

- Whether FirstEnergy was in violation of NRC cyber-security regulations at the time of the worm attack.
- Whether there is any evidence that last week's blackout could have been caused or exacerbated by the Blaster worm or some other cyber-security flaw, and whether a cyber-attack could successfully penetrate nuclear reactor networks and result in an outage of that reactor and/or a more widespread outage.

# # #